Consumentenrecht en cybersecurity

Verbruggen, Paul

Published in:
Tijdschrift voor consumentenrecht & handelspraktijken

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Van de redactie

Voor u ligt de derde aflevering van *TvC* van dit jaar. In een eerder redactioneel stonden wij kort stil bij actuele ontwikkelingen en het consumentenrecht, meer specifiek de deeleconomie. Wij nodigden daarbij auteurs uit om met een bijdrage over de deeleconomie te komen. Daar werd gehoor aan gegeven. In deze aflevering ziet u daar het eerste resultaat van in de vorm van een interessante uiteenzetting van De Vries over de positie van 'taxibedrijf' Uber in relatie tot consumenten. In de tweede helft van 2016 zult u nog andere bijdragen over de deeleconomie terugvinden in *TvC*. Tegelijkertijd dienen zich alweer nieuwe ontwikkelingen aan voor het Nederlands en Europees consumentenrecht, zoals de conformiteit van producten en diensten in het licht van digitale (on)veiligheid.

Actuele ontwikkelingen: consumentenrecht en cybersecurity

Waartoe zijn consumenten gerechtigd als blijkt dat de door hen aangeschafte goederen met ICT-toepassingen of digitale diensten onveilig zijn in termen van cybersecurity? Die vraag stond centraal in een belangwekkende procedure die de Consumentenbond onlangs aanspande tegen telefoongigant Samsung.[1] Kort gezegd draaide de betreffende kortgedingprocedure om het volgende. In juli 2015 werd bekend dat in Google's besturingssysteem Android een beveiligingslek (een 'bug') zat. Deze bug, genaamd *Stagefright*, maakte het mogelijk om smartphones die draaien op dit systeem te hacken waardoor de hacker zich toegang kon verschaffen tot de data op de telefoon en de microfoon en camera op deze toestellen op afstand kon bedienen om zo gebruikers te bespioneren. In oktober 2015 werd een tweede versie van het lek (*Stagefright 2.0*) aangekondigd.[2] De smartphones van Samsung draaien op het Android-besturingssysteem en als gevolg daarvan blijkt een aantal wat oudere, maar nog steeds veel verkochte Samsung-modellen kwetsbaar te zijn voor cyberaanvallen. Hoewel Google reeds een aantal 'patches' ter beschikking stelde om de kwetsbaarheid te verhelpen, voerde Samsung die patches niet door op de kwetsbare toestellen. Ze informeerde haar Nederlandse consumenten zelfs niet over de bug.

De Consumentenbond startte derhalve een civiele verbodsactie voor de Voorzieningenrechter te Amsterdam waarin ze onder meer vorderde dat Samsung de gebruikers van haar kwetsbare smartphones zal informeren over de *Stagefright*-bug, dat zij de veiligheidsupdates die Google als kritisch beschouwd doorvoert voor de modellen die deze bug hebben, en dat zij voor alle smartphonemodellen geïntroduceerd in Nederland in de laatste twee jaar, alsmede die in de toekomst, van beveiligingsupdates zal blijven voorzien. Volgens de Consumentenbond heeft Samsung in Nederland een aandeel van meer dan 40% op de smartphonemarkt, terwijl zo'n 80% van haar Smartphones kwetsbaar blijken voor de *Stagefright*-bug.

De procedure loopt voor Samsung met een sisser af, voorlopig dan. De voorzieningenrechter oordeelt namelijk dat de Consumentenbond faalt in haar bewijs ten aanzien van het spoedeisend belang in de onderhavige zaak. Het blijkt namelijk dat de kwetsbaarheid als gevolg van de *Stagefright*-bug in de praktijk zeer moeilijk uit te buiten valt. Android-smartphones zijn nog slechts in een testomgeving gekraakt en niet '*in the wild*'. Het risico dat de consument volgens de Consumentenbond aldus loopt, is onvoldoende om de toets van spoedeisend belang in kort geding te doorstaan.

Bijgevolg oordeelt de voorzieningenrechter niet over een aantal uiterst belangrijke materiële vragen die spelen in deze zaak. Die vragen zijn onder meer:

i. Is een producent, aanbieder of verkoper van goederen met ICT-toepassingen (zoals de smartphones van Samsung) gehouden om updates of upgrades te verschaffen aan gebruikers van deze goederen en diensten indien blijkt dat deze toepassingen (ICT-systemen, infrastructuur, software, firmware, enz.) beveiligingslekken bevatten en dus geen cybersecurity bieden voor gebruikers?
ii. Bestaat een dergelijke verplichting ongeacht het feit dat de kwetsbare ICT-toepassing (Android) wordt geleverd door een derde (Google)?
iii. Binnen welke tijdsspanne zou een dergelijke verplichting bestaan? Zou men slechts binnen een korte periode nadat het product op de markt is gebracht updates of upgrades moeten verschaffen? Of zou dat voor de normale levensduur van de goederen zijn? Of zelfs voor de gehele 'life cycle' van het product?
iv. Is het risico dat een ICT-toepassing gehackt kan worden al voldoende om een verplichting tot updaten of upgraden te laten bestaan, ook al heeft dit risico zich nog niet in werkelijkheid voorgedaan?
v. Moet een aanbieder of verkoper van goederen met ICT-toepassingen de consument informeren over wat hij of zij kan verwachten in termen van cybersecurity voordat een overeenkomst met de consument gesloten wordt?
vi. Kunnen aanbieders of verkopers van goederen met ICT-toepassingen hun eventuele aansprakelijkheid voor schade veroorzaakt door een beveiligingslek in de goederen beperken of uitsluiten via hun algemene voorwaarden?

1. Rb. Amsterdam (pres.) 8 maart 2016, C/13/600958/KG ZA 16/51.
2. www.theguardian.com/technology/2015/jul/28/stagefright-android-vulnerability-heartbleed-mobile (laatst geraadpleegd op 9 mei 2016).

Deze vragen raken stuk voor stuk kernleerstukken van het consumentenrecht en meer in het algemeen het verbintenissenrecht. Zij doen zich overigens niet alleen voor ten aanzien van goederen met ICT-toepassingen, maar zijn ook bij diensten van de informatiemaatschappij en zogenaamde 'digitale inhoud' zeer relevant.[3] Ook in het licht van de voortschrijdende ontwikkeling van het '*internet of things*' zijn deze vragen pertinent nu deze ontwikkeling een geïntegreerd netwerk van 'things' voorstaat waarin objecten onafhankelijk van menselijk ingrijpen met elkaar communiceren, persoonsgegevens verzamelen, delen en verwerken en aldus diensten aanbieden aan consumenten.[4] Een beveiligingslek in een van deze objecten maakt infiltratie in het gehele netwerk mogelijk. Bovendien beschikken de objecten waar het in het internet of things om gaat, zoals slimme thermostaten, weegschalen, koelkasten en kledingstukken, vooralsnog niet over voldoende energie- en computercapaciteit om een hoog niveau van veiligheid te waarborgen, waardoor cyberaanvallen uiterst effectief kunnen zijn.[5]

Naar verluidt zal de Consumentenbond een bodemprocedure starten waarin de rechter zich niet zo gemakkelijk aan de opgesomde vragen zal kunnen onttrekken als de voorzieningenrechter dat deed. De vragen zijn tot nu toe nog maar nauwelijks aan de orde gekomen in procedures in Nederland (en daarbuiten) en de te verwachten bodemprocedure zal daarom kritisch worden gevolgd. De tijd lijkt rijp voor een aantal principiële uitspraken over deze problematiek zodat meer rechtszekerheid wordt geboden over de vraag waartoe consumenten gerechtigd zijn als blijkt dat de door hen aangeschafte goederen met ICT-toepassingen en digitale diensten 'cyber *in*secure' zijn. Nu de beantwoording van deze vraag ongetwijfeld brede repercussies zal hebben voor de veelal internationale ICT-sector, is het wellicht ook verstandig om te bezien of wetgevingsinitiatieven op Europees niveau wenselijk zijn om tot een meer uniform juridisch kader te komen inzake het consumentenrecht en cybersecurity.

Inhoud aflevering 3, 2016

In deze aflevering volgt allereerst de bijdrage van Anne de Vries over de positie van de innovatieve taxi-app Uber. Dit 'vervoerbedrijf' timmert wereldwijd stevig aan de weg, maar doet daarbij wel regelmatig het nodige stof opwaaien. Opvallend is dat er vanuit de rechtswetenschap nog betrekkelijk weinig onderzoek gedaan is naar de juridische positie van Uber in relatie tot haar consumenten. De Vries buigt zich als een van de eerste onderzoekers over de vraag of Uber een aanbieder van een taxidienst, een bemiddelaar of niet meer dan een digitaal prikbord is. Vervolgens treft u in deze aflevering een uitgebreide kroniek aan. Marco Loos heeft zich met volle overtuiging op de ontwikkelingen rondom de reisovereenkomst gestort. Daarbij keek hij naar de periode 2012-2015. Daarmee sluit hij mooi aan bij zijn eerdere kroniek over de periode 2008-2012 uit *TvC* 2013, afl. 1. Naast het bespreken van de belangrijkste uitspraken staat Loos in zijn kroniek stil bij de nieuwe Richtlijn pakketreizen uit 2015. Naast deze twee artikelen bevat deze aflevering ook twee annotaties. In 2015 wees de Rechtbank Amsterdam vonnis in twee gevoegde zaken waarbij twee claimstichtingen tegen ABN AMRO procedeerden over Euribor-hypotheken die de bank aan consumenten had verkocht. Centraal stond de vraag of het heffen van een opslagpercentage bovenop de Euribor-rente in strijd is met de algemene-voorwaardenregeling. Vaste medewerker van dit tijdschrift Jan Spanjaard laat zijn licht over deze uitspraken schijnen. Daarnaast treft u een annotatie van Loos aan bij de zaak *Verein für Konsumenteninformation/A1 Telekom Austria* van het Hof van Justitie EU. Deze uitspraak brengt een belangrijke nuancering aan op de arresten *RWE, Kásler* en *Schulz* uit 2013 en 2014.[6] Loos legt u in zijn noot precies uit hoe dit zit.

Vanessa Mak en, wederom, Loos bespreken in deze aflevering ook nog diverse boeken die relevant zijn voor de bestudering van het consumentenrecht. Zo bespreekt Mak onder andere de nieuwe Asser Vermogensrecht Algemeen. Europees recht en Nederlands vermogensrecht van Hartkamp en gaat Loos in op enkele boeken die zich richten op digitale overeenkomsten alsmede 'social media'. Tevens treft u in deze aflevering zoals gebruikelijk de rubriek van Bregje Krijnen aan. Dit keer staat zij stil bij twee prikkelende uitspraken. Het blijkt dat het deelnemen aan een televisieprogramma niet voor iedereen een fijne ervaring oplevert. Zo willen deelnemers van illustere programma's als Idols en Mijn Leven in Puin nog wel eens via de rechter proberen om uitzending van die programma's te voorkomen. Naast secundaire victimisatie van de teleurgestelde programmadeelnemers leverden deze zaken ook de nodige inspiratie op voor Krijnen. Wij sluiten deze aflevering af met de laatste ontwikkelingen op wetgevingsgebied door middel van de Wettenagenda van onze vaste medewerkster Sarah van Kampen. Van Kampen bespreekt onder andere het recente Wetsvoorstel consumentenkredietovereenkomsten, goederenkrediet en geldlening en de voor de digitale consument relevante Verordening portabiliteit.

Rest ons niets dan u veel leesplezier te wensen!

Mr. dr. P.W.J. Verbruggen

3. 'Digitale inhoud' is een verzamelbegrip waar onder meer video, audio, applicaties, digitale games, software en cloudcomputing onder vallen. Cf. artikel 2(1) van het Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud, COM(2015)634 final, Brussel: 9 december 2015.
4. Zie in het algemeen over deze ontwikkeling C. Prins, 'Mijn intelligente koelkast', *NJB* 2015, afl. 23, p. 1519.
5. Zo waarschuwt het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders, de Artikel 29-werkgroep, dat: 'As their components use wireless communications infrastructures and are characterised by limited resources in terms of energy and computing power, devices [connected in the Internet of Things – IoT] are vulnerable to physical attacks, eavesdropping or proxy attacks. Most common technologies currently in use – i.e. KPI infrastructures – are not easily ported on IoT devices since most of the devices do not have the computing power needed to cope with the required processing tasks. Artikel 29-werkgroep, 'Opinion 8/2014 on the recent developments on the Internet of Things' 14/EN, WP 223, Opinie van 16 september 2014.
6. HvJ 21 maart 2013, C-92/11, ECLI:EU:C:2013:180 (*RWE*); HvJ 30 april 2014, C-26/13, ECLI:EU:C:2014:282 (*Kásler en Káslerné Rábai/OTP Jelzálogbank Zrt*); HvJ 23 oktober 2014, gevoegde zaken C-359/11 en C-400/11, ECLI:EU:C:2014:2317 (*Schulz/Technische Werke Schussental* en *Egbringhoff/Stadtwerke Ahaus*).